Приложение № 1

УТВЕРЖДЕНА
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № _81

ПОЛИТИКА

администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-фз «О персональных данных»

Агалатово
2021

ОПРЕДЕЛЕНИЯ

Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных).

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых оператором с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники оператора.

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных - совокупность содержащихся в базах данных оператора персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1. Общие положения

1.1 Правовая основа

Политика администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее Политика):

- Трудового кодекса Российской Федерации;
- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- постановления Правительства Российской Федерации от 21.03.2012 № 211 «Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

Настоящая Политика устанавливает единый порядок обработки персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

1.2 Цель Политики

Целью настоящей Политики является обеспечение безопасности персональных данных граждан от несанкционированного доступа, неправомерного их использования или утраты.

Настоящая Политика устанавливает и определяет:

- процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных;
- цели обработки персональных данных;
- перечень обрабатываемых персональных данных;
- категории субъектов, персональные данные которых обрабатываются;
- сроки обработки и хранения обрабатываемых персональных данных;
- порядок уничтожения обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований;
- правила рассмотрения запросов субъектов персональных данных или их представителей;
- правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к обеспечению безопасности персональных данных, установленных Федеральным законом № 152-ФЗ, принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области;
- правила работы с обезличенными данными;
- перечень информационных систем персональных данных;
- перечень должностей муниципальных служащих администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных;
- перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным;
- ответственного за организацию обработки персональных данных;

- обязательство лица, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним трудового договора (контракта) прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей;

- типовую форму согласия на обработку персональных данных субъектов персональных данных;

- порядок доступа в помещения, в которых ведется обработка персональных данных.

1.3 Основные условия обработки персональных данных

Обработка персональных данных осуществляется после принятия необходимых мер по обеспечению безопасности персональных данных, а именно:

- после получения согласия субъекта персональных данных, в соответствии с частью 2 статьи 6 Федерального закона № 152-ФЗ;

- после направления уведомления об обработке персональных данных в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, за исключением случаев, предусмотренных частью 2 статьи 22 Федерального закона от 27.07.2006 № 152-ФЗ;

Лица, допущенные к обработке персональных данных, под роспись знакомятся с настоящей Политикой и подписывают обязательство о неразглашении информации, содержащей персональные данные.

2. Процедуры, направленные на выявление и предотвращение нарушений законодательства в сфере персональных данных

2.1. Меры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации

К мерам, направленным на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных относятся:

- назначение ответственного за организацию обработки персональных данных;

- применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии с частями 1 и 2 статьи 19 Федерального закона № 152-ФЗ;

- осуществление внутреннего контроля соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами, требованиями к обеспечению безопасности персональных данных, политике и локальным актам администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в отношении обработки персональных данных;

- оценка вреда, который может быть причинен субъектам персональным данных в случае нарушения законодательства Российской Федерации и настоящего Положения;

- ознакомление работников, непосредственно осуществляющих обработку персональных данных с положениями законодательства Российской Федерации о персональных данных и настоящим Положением;

- запрет на обработку персональных данных лицами, не допущенными к их обработке.

Документы, определяющие политику администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в отношении обработки персональных данных, подлежат обязательному опубликованию.

2.2. Порядок обработки персональных данных в информационных системах персональных данных с использованием средств автоматизации

Обработка персональных данных в информационных системах персональных данных с использованием средств автоматизации осуществляется в соответствии с требованиями постановления Правительства Российской Федерации от

01.10.2012 № 1119 «Об утверждении требований к защите персональных данных при обработке в информационных системах персональных данных», нормативных и руководящих документов уполномоченных федеральных органов исполнительной власти.

При эксплуатации автоматизированных систем необходимо соблюдать требования:

- к работе допускаются только лица, назначенные распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области;
- на ПЭВМ, на которых обрабатываются и хранятся сведения о персональных данных, должны быть установлены пароли (идентификаторы);
- на период обработки защищаемой информации в помещении должны находиться только лица, допущенные в установленном порядке к обрабатываемой информации; допуск других лиц в указанный период может осуществляться с разрешения главы муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

2.3. Порядок обработки персональных данных без использования средств автоматизации

Обработка персональных данных без использования средств автоматизации (далее - неавтоматизированная обработка) может осуществляться в виде документов на бумажных носителях.

При неавтоматизированной обработке различных категорий персональных данных должен использоваться отдельный материальный носитель для каждой категории персональных данных.

При неавтоматизированной обработке персональных данных на бумажных носителях:

- не допускается фиксация на одном бумажном носителе персональных данных, цели обработки которых заведомо несовместимы;
- персональные данные должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков);
- документы, содержащие персональные данные, формируются в дела в зависимости от цели обработки персональных данных;
- дела с документами, содержащими персональные данные, должны иметь внутренние описи документов с указанием цели обработки и категории персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовые формы), должны соблюдаться следующие условия:

- типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки персональных данных, имя (наименование) и администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых администрацией муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области способов обработки персональных данных;
- типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на неавтоматизированную обработку персональных данных, - при необходимости получение письменного согласия на обработку персональных данных;
- типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов

персональных данных;

- типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо несовместимы.

Документы и внешние электронные носители информации, содержащие персональные данные, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах). При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность.

Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

- при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

- при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации, а том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3. Цели обработки персональных данных

Целями обработки персональных данных являются:

- организация деятельности администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области для обеспечения соблюдения законов и иных нормативно-правовых актов, реализации права на труд;

- осуществления, возложенных на администрацию муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области функций, полномочий и обязанностей в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций.

4. Сроки обработки и хранения обрабатываемых персональных данных

4.1. Сроки обработки и хранения обрабатываемых персональных данных

Сроки обработки и хранения персональных данных определяются:

- Приказом Росархива от 20.12.2019 № 236 «Об утверждении Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков их хранения»;
- сроком исковой давности;
- иными требованиями законодательства Российской Федерации и муниципальными нормативно-правовыми актами администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

4.2. Особенности хранения персональных данных

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных.

5. порядок уничтожения обработанных персональных данных

5.1. Уничтожение обработанных персональных данных при достижении целей обработки или при наступлении иных законных оснований

Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обрабатываемые персональные данные подлежат уничтожению по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

5.2. Порядок уничтожения обработанных персональных данных

Уничтожение обработанных персональных данных производится комиссией с составлением соответствующего акта.

6. Правила рассмотрения запросов субъектов персональных данных

Правила рассмотрения запросов субъектов персональных данных оформляются отдельным документом и утверждаются главой муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

7. Ответственный за организацию обработки персональных данных

7.1. Ответственный за организацию обработки персональных данных

Ответственный за организацию обработки персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области назначается распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области из числа сотрудников администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

7.2. Инструкция ответственного за обработку персональных данных

Инструкция ответственного за обработку персональных данных утверждается распоряжением администрации муниципального образования

«Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области. Ответственный за организацию обработки персональных под роспись знакомиться с инструкцией ответственного за организацию обработки персональных данных.

8. Перечень должностей, осуществляющих обработку персональных данных

8.1. Перечень должностей

Перечень должностей муниципальной службы, при замещении которых служащие допускаются к обработке персональных данных и имеют доступ к персональным данным, утверждается распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

8.2. Обязательство о неразглашении персональных данных

Лица, допущенные к обработке персональных данных, в обязательном порядке под роспись знакомятся с настоящими Правилами и подписывают обязательство о неразглашении информации, содержащей персональные данные.

9. Правила работы с обезличенными данными

Правила работы с обезличенными персональными данными оформляются отдельным документом и утверждаются распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

10. Ответственность за проведение мероприятий по обезличиванию персональных данных

Перечень должностей, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных оформляется отдельным документом и утверждается распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

11. Порядок доступа в помещения, в которых ведётся обработка персональных данных

Порядок доступа в помещения, в которых ведётся обработка персональных данных оформляется в виде отдельного документа и утверждается распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

12. Правила осуществления внутреннего контроля

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к обеспечению безопасности персональных данных оформляются отдельным документом и утверждаются распоряжением администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

Приложение 2

УТВЕРЖДЕНО

распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № _81

ПОЛОЖЕНИЕ

об обеспечении безопасности персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

д. Агалатово
2021 г.

1. Термины и определения

В настоящем Положении использованы следующие термины и определения:

Безопасность персональных данных: Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных: Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вирус (компьютерный, программный): Исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносное программное обеспечение: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации: Возможность получения информации и ее использования.

Защита информации: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защищаемая информация: Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация: Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных (ИСПДн): Информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таковых средств.

Информационные технологии: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способ осуществления таких процессов и методов.

Информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Использование персональных данных: Действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом, затрагивающих права и свободы субъекта персональных данных или других лиц.

Конфиденциальная информация: Информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

Криптографическая защита: Защита информации от ее несанкционированной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования.

Межсетевой экран: Локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс),

реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности: Функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Обезличивание персональных данных: Действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных: Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор персональных данных (оператор): Муниципальный орган, организующий и (или) осуществляющий обработку ПДн, а также определяющие цели и содержание обработки ПДн.

Персональные данные (ПДн): Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Предоставление информации: Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.

Разграничение доступа (правила разграничения доступа): Совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Распространение персональных данных: Действия, направленные на передачу ПДн определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Средство вычислительной техники: Совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Технические средства информационной системы персональных данных: Средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео - и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации).

Угрозы безопасности персональных данных: Совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных: Действия, в результате которых невозможно восстановить содержание персональных данных в ИСПДн или в

результате которых уничтожаются материальные носители персональных данных.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Шифрование: Процесс преобразования открытой информации с целью сохранения ее в тайне от посторонних лиц при помощи некоторого алгоритма, называемого шифром.

Электронный документ: Документ, в котором информация представлена в электронно-цифровой форме. Электронный документ может создаваться на основе документа на бумажном носителе, на основе другого электронного документа либо порождаться в процессе информационного взаимодействия.

Электронная подпись: Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

2. Используемые сокращения

В настоящем Положении использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	Описание
1.	**ИСПДн**	Информационная система персональных данных
2.	**НСД**	Несанкционированный доступ
3.	**ПДн**	Персональные данные
4.	**СКЗИ**	Средство криптографической защиты информации
5.	**СЗПДн**	Система защиты персональных данных

3. Область применения

Настоящее Положение об обеспечении безопасности персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области (далее - Положение) предназначено для применения при организации и проведении работ по обеспечению безопасности персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области (далее по тексту - Администрация).

Требования настоящего Положения распространяются на сотрудников Администрации, принимающих участие в обеспечении безопасности персональных данных.

4. Общие положения

Настоящее Положение определяет содержание и порядок осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных (ИСПДн) Администрации, представляющей собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных как с использованием средств автоматизации, так и без использования таких средств.

Безопасность персональных данных при их обработке в ИСПДн достигается путем снижения вероятности осуществления НСД к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

При обработке персональных данных в ИСПДн Администрации должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение НСД к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов НСД к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
- непрерывный контроль и анализ уровня защищенности персональных данных.

Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные мероприятия и средства защиты информации (в том числе криптографические средства, средства предотвращения НСД, программно-технических воздействий на технические средства обработки ПДн), а также используемые в ИСПД информационные технологии.

Обеспечение безопасности персональных данных в Администрации осуществляется на основе следующих принципов:

- соответствие мер и средств защиты актуальным угрозам безопасности - построение и модернизация СЗПДн в Администрации производится на основе анализа угроз безопасности персональных данных с учетом специфических особенностей ИСПДн;
- соответствие мер и средств защиты требованиям нормативных документов РФ - в Администрации используются меры и средства обеспечения безопасности персональных данных в строгом соответствии с действующими нормативными правовыми актами РФ в области обработки и защиты персональных данных;
- комплексность - с целью обеспечения безопасности персональных данных в Администрации используется совокупность организационных мер и технических средств защиты;
- патентная чистота - средства защиты информации, входящие в состав СЗПДн, отвечают требованиям по обеспечению патентной чистоты согласно действующим нормативным документам РФ. Используемое общесистемное, специальное и прикладное программное обеспечение имеет соответствующие лицензии производителей.
- удобство пользователей - при построении и модернизации СЗПДн учитываются и по возможности сводятся к минимуму возможные трудности пользователей в работе со средствами защиты и с основными процедурами обеспечения безопасности персональных данных;
- постоянное совершенствование - осуществляется регулярный внутренний контроль выполнения требований по обработке и обеспечению безопасности персональных данных, эффективности применяемых организационных мер и технических средств защиты и уровня защищенности персональных данных, а также регулярно пересматриваются состав угроз и уровень защищенности ПДн, на основании чего принимаются меры по устранению выявленных недостатков и модернизации/совершенствованию СЗПДн.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в ИСПДн оценивается при проведении государственного контроля и надзора.

Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн Администрации включают в себя:

- определение уровня защищенности обрабатываемых ПДн, в том числе отслеживание изменений состояния ИСПДн, которые могут повлиять на классификационные признаки ИСПДн (уровень защищенности ПДн);
- определение угроз безопасности персональных данных при их обработке в ИСПДн;
- разработка на основании определенных угроз и поддержание в актуальном состоянии частной модели безопасности угроз безопасности персональных данных при обработке их в ИСПДн;
- разработку на основе частной модели угроз системы защиты персональных данных (СЗПДн), обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для установленного уровня защищенности ПДн;
- установку и ввод в эксплуатацию СЗИ, входящих в состав СЗПДн, в соответствии с проектными решениями по созданию СЗПДн, эксплуатационной и технической документацией к данным СЗИ;
- обучение лиц, использующих СЗИ, входящие в состав СЗПДн, правилам работы с ними;
- учет применяемых СЗИ, входящих в состав СЗПДн, эксплуатационной и технической документации к ним;
- учет носителей персональных данных;
- учет лиц, допущенных к работе с персональными данными в ИСПДн;
- контроль соблюдения условий использования СЗИ, входящих в состав СЗПДн, предусмотренных эксплуатационной и технической документацией к ним;
- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования СЗИ, входящих в состав СЗПДн, которые могут привести к нарушению заданных характеристик безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
- описание состава и режима функционирования компонентов СЗПДн (описание СЗПДн).

Размещение компонентов ИСПДн, охрана помещений, в которых ведется работа с персональных данных, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и СЗИ, входящих в состав СЗПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

Настоящее Положение должно быть доведено до всех работников Администрации, участвующих в обеспечении безопасности персональных данных, под роспись.

5. Стадии создания СЗПДН

В Администрации обеспечение безопасности персональных данных осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках следующих стадий создания и совершенствования СЗПДн:

- предпроектная стадия;
- стадия проектирования;
- стадия приемки и ввода в действие;
- модернизация СЗПДн.

СЗПДн включает организационные меры, технические средства защиты информации, а также используемые в ИСПДн информационные технологии, реализующие функции защиты информации.

Выполнение всех вышеуказанных стадий должно проходить по согласованию с должностным лицом, ответственным за организацию работ по обработке персональных данных.

Выполнение всех вышеуказанных стадий должно проходить под контролем должностного лица, ответственным за проведение работ по защите персональных данных.

5.1. Описание требований к предпроектной стадии создания СЗПДн

Целью предпроектной стадии создания СЗПДн является:

- определение категории субъектов персональных данных, чьи данные обрабатываются в Администрации, состава и объема обрабатываемых персональных данных, а также цели и правовое основание обработки этих данных;
- определение должностных лиц, участвующих в обработке персональных данных;
- определение угроз безопасности персональных данных применительно к конкретным условиям функционирования ИСПДн;
- определение уровня защищенности ПДн.

Для достижения указанных целей проводится анализ информационных систем Администрации, содержащих персональные данные, и определяются все внутренние и внешние процессы обработки персональных данных, осуществляемые как с использованием средств автоматизации, так и без использования таковых.

По результатам предпроектной стадии определяется степень выполнения требований нормативно-правовых документов в области защиты персональных данных, а также разрабатывается план необходимых дальнейших организационных и технических мероприятий по реализации данных требований.

Должностное лицо, ответственное за проведение работ по защите персональных данных, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели предпроектной стадии.

5.1.1. Определение обрабатываемых персональных данных

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в Администрации определяются состав, цели, правовое основание обработки персональных данных и сроки хранения обрабатываемых персональных данных.

На основании полученных данных формируется документ «Перечень персональных данных, обрабатываемых в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

5.1.2. Определение перечня должностных лиц, допущенных к работе с персональными данными

В ходе предпроектной стадии по результатам анализа процессов обработки персональных данных в Администрации определяется перечень лиц, которым необходим доступ к персональных данных для выполнения трудовых обязанностей, а также перечень лиц, которые в рамках выполнения своих трудовых обязанностей имеют право доступа к ресурсам, содержащим персональные данные, без права ознакомления с персональными данными.

На основании полученных данных формируется перечень должностных лиц, допущенных в помещения и к работе со средствами вычислительной техники из состава ИСПДн Администрации, который утверждается соответствующим распоряжением администрации.

5.1.3. Определение конфигурации и топологии ИСПДн

В ходе обследования информационных систем Администрации определяются все базы данных (хранилища) и отчуждаемые носители информации и содержащиеся в них персональных данных. Кроме того, определяются конфигурация и топология ИСПДн в целом и ее отдельных компонентов, а именно перечень серверного оборудования, автоматизированных рабочих мест, общесистемных и прикладных программных средств,

задействованных при обработке персональных данных, перечень применяемых средств защиты информации, а также сетевая инфраструктура и перечень сетевого оборудования.

5.1.4. Определение угроз безопасности персональных данных

С целью определения необходимых мер и средств защиты, соответствующих актуальным угрозам безопасности персональных данных при их обработке в ИСПДн Администрации, проводится анализ и оценка вероятности реализации и величины негативных последствий вследствие реализации угроз безопасности персональных данных при их обработке в ИСПДн.

В Администрации составляется частная модель угроз безопасности персональных данных, которая разрабатывается на основании:

- ГОСТ Р 51275-2006 «Защита информации. Факторы, воздействующие на информацию. Общие положения»;
- Базовой модели угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 15 февраля 2008 г. заместителем директора ФСТЭК России;
- Методики определения актуальных угроз безопасности персональных данных при обработке в информационных системах персональных данных, утвержденной 14 февраля 2008 г. заместителем директора ФСТЭК России;
- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54-144.

5.1.5. Определение уровня защищенности ПДн

Определение уровня защищенности ПДн осуществляется в соответствии с требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». При определении уровня защищенности ПДн используется модель угроз безопасности ПДн, в которой проведен анализ актуальных угроз безопасности ПДн.

5.2. Стадия проектирования СЗПДн

Цели проектирования СЗПДн:

- определить требования по обеспечению безопасности персональных данных;
- определить структуру и характеристики создаваемой СЗПДн, состав технических средств защиты информации, предполагаемых к использованию в СЗПДн, требования к настройке и эксплуатации этих средств, параметры их взаимодействия, а также план мероприятий по подготовке СЗПДн к вводу в действие;
- определить требования и регламентировать деятельность работников Администрации по организации легитимной обработки персональных данных и обеспечению безопасности персональных данных, обрабатываемых как с использованием средств автоматизации, так и без использования таковых.

Для достижения указанных целей в Администрации разрабатывается комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.

Должностное лицо, ответственное за проведение работ по защите персональных данных в Администрации, определяет необходимость проведения мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии проектирования СЗПДн.

5.2.1. Определение требований по обеспечению безопасности персональных данных

По результатам предпроектной стадии, в зависимости от определенного уровня защищенности ПДн и определенного перечня актуальных угроз безопасности персональных данных, задаются конкретные требования по обеспечению безопасности ПДн при их обработке в ИСПДн Администрации, выполнение которых обеспечивает минимизацию вероятности реализации предполагаемых угроз безопасности персональных данных.

5.2.2. Определение конфигурации СЗПДн

На основании требований, указанных выше, осуществляется проектирование СЗПДн, определяется состав и характеристики средств защиты информации, которые будут входить в состав создаваемой СЗПДн.

В Администрации разрабатывается комплект организационно-распорядительной документации на СЗПДн, описывающей требования и процедуры по управлению и обеспечению безопасности персональных данных. За разработку и, при необходимости, пересмотр организационно-распорядительной документации на СЗПДн в Администрации отвечает должностное лицо, ответственное за проведение работ по обеспечению безопасности персональных данных в Администрации.

5.3. Стадия ввода в действие СЗПДн

Цели стадии ввода в действие СЗПДн:

- внедрить технические средства защиты информации;
- проверить работоспособность средств защиты информации в составе ИСПДн;
- принять организационные меры по обеспечению безопасности персональных данных;
- ознакомить работников Администрации с требованиями и обучить порядку обработки и обеспечения безопасности персональных данных.

Для достижения перечисленных целей выполняются следующие мероприятия:

- осуществляется закупка, установка и настройка средств защиты информации;
- проводятся опытная эксплуатация и приемо-сдаточные испытания средств защиты информации;
- утверждается и вводится в действие комплект организационно-распорядительных документов, определяющих требования и порядок действий при обработке и обеспечении безопасности персональных данных.
- проводится обучение работников по направлению обеспечения безопасности персональных данных.
- Должностное лицо, ответственное за проведение работ по защите персональных данных в Администрации, определяет необходимость проведения тех или иных мероприятий, направленных на достижение перечисленных целей, и является ответственным за организацию и планирование действий, в результате которых достигаются цели стадии ввода в действие СЗПДн.

5.3.1. Внедрение средств защиты информации

Согласно требованиям, определенным в документации, осуществляется закупка, установка и настройка программных и технических средств защиты информации с составлением соответствующих актов установки.

Установка и ввод в эксплуатацию средств защиты информации осуществляется строго в соответствии с эксплуатационной и технической документации к ним. Перед установкой средств защиты информации проверяется их готовность к использованию, и составляются заключения о возможности их эксплуатации.

В Администрации необходимо применять средства защиты информации, прошедшие в установленном порядке процедуру оценки соответствия и имеющие соответствующие сертификаты ФСТЭК и ФСБ России.

5.3.2. Внедрение организационных мер по обеспечению безопасности персональных данных

В Администрации утверждается и вводится в действие комплект организационно-распорядительной документации на СЗПДн.

Все должностные лица, допущенные к обработке персональных данных, и лица, ответственные за обеспечение безопасности персональных данных, в обязательном порядке изучают организационно-распорядительные документы на СЗПДн в части их касающейся и руководствуются ими в своей работе.

Общий контроль над исполнением требований организационно-распорядительной документации на СЗПДн в Администрации возлагается на должностное лицо, ответственное за обеспечение безопасности ПДн.

5.3.3. Обучение работников по направлению обеспечения безопасности персональных данных

В Администрации все работники, участвующие в обработке персональных данных, в обязательном порядке проходят обучение по следующим направлениям:

- общие вопросы обеспечения информационной безопасности;
- правила автоматизированной и неавтоматизированной обработки персональных данных и обеспечения безопасности персональных данных;
- правила использования прикладных систем и технических средств обработки персональных данных;
- правила использования средств защиты информации, входящих в состав СЗПДн;
- ответственность за нарушение правил обработки и обеспечения безопасности персональных данных.

Ответственным за организацию и контроль проведения обучения работников Администрации, участвующих в обработке и обеспечении безопасности персональных данных, является должностное лицо, ответственное за обеспечение безопасности персональных данных в Администрации.

Обучение может проводиться как самим должностным лицом, ответственным за обеспечение безопасности персональных данных в Администрации, так и с привлечением сторонних организаций.

Новые работники Администрации, принимаемые на работу, в обязательном порядке проходят первичный инструктаж. Ответственным за направление работника на первичный инструктаж является должностное лицо, ответственное за организацию работ по обработке персональных данных в Администрации.

Перед допуском работников Администрации к работе с ПДн должностное лицо ответственное за обеспечение безопасности ПДн проводит ознакомление с нормативной документацией, утвержденной в Администрации, в области безопасности ПДн.

5.4. Модернизация СЗПДн

В случаях изменения состава или структуры ИСПДн Администрации, состава угроз безопасности персональных данных или уровня защищенности ПДн, обработка которых осуществляется в ИСПДн Администрации, проводится модернизация СЗПДн.

6. Мероприятия по организации и обеспечению безопасности персональных данных

Под организацией обеспечения безопасности персональных данных при их обработке в ИСПДн Администрации понимается формирование и реализация совокупности согласованных по целям, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности персональных данных.

Организационные мероприятия по обеспечению безопасности персональных данных в Администрации включает в себя:

- мероприятия по обеспечению охраны и физической защиты помещений, в которых расположены технические средства ИСПДн, исключающие несанкционированный доступ к техническим средствам ИСПДн, их хищение и нарушение работоспособности;
- обучение работников Администрации правилам обработки и защиты персональных данных.

В целях осуществления технического обеспечения безопасности персональных данных при их обработке в ИСПДн Администрации реализовываются мероприятия по защите от НСД к ПДн.

Планирование мероприятий по обеспечению безопасности персональных данных осуществляется в соответствии с Разделом 8 настоящего Положения.

6.1. Мероприятия по обеспечению управления доступом

6.1.1. Общие требования

Для организации системы допуска и учета должностных лиц, допущенных к работе с персональными данными в Администрации, должен быть определен перечень должностных лиц и утвержден соответствующим распоряжением главы администрации.

В Администрации должна быть реализована разрешительная система допуска пользователей и разграничение прав доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации с помощью функциональных возможностей операционной системы, прикладных систем обработки персональных данных либо специализированных средств защиты информации.

Работникам Администрации предоставляется доступ к ПДн и средствам их обработки в объеме, минимально необходимом для выполнения их трудовых обязанностей.

Для идентификации и аутентификации пользователей ИСПДн Администрации должны применяться пароли условно-постоянного действия. Требования к формированию пароли и периодичности их смены определены в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности, и Инструкция работника по правилам обработки ПДн).

6.1.2. Порядок проведения мероприятий

Своевременное предоставление работникам Администрации прав доступа к персональным данным и средствам их обработки, а также изменение их полномочий обеспечивает должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации.

Порядок генерации, смены и прекращения действия паролей в ИСПДн Администрации определен в эксплуатационной документации на СЗПДн).

6.2. Мероприятия по обеспечению регистрации и учета

6.2.1. Учет и хранение носителей ПДн

6.2.1.1. Требования

В Администрации должен вестись учет как машинных, так и бумажных носителей ПДн. Также должно быть организовано хранение и использование этих носителей, исключающее их хищение, подмену и уничтожение.

В Администрации учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD, BD и прочее);
- неотчуждаемые носители информации (жесткие магнитные диски).

6.2.1.2. Порядок проведения мероприятий

Порядок учета, хранения, использования носителей персональных данных (машинных и бумажных), а также порядок их уничтожения определены в документе «Порядок учета, хранения и уничтожения носителей персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

Ответственность за ведение учета машинных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей

персональных данных возлагается на должностное лицо, ответственное за защиту ПДн.

Контроль и ответственность за ведение учета бумажных носителей персональных данных, организацию надлежащего хранения, а также уничтожение носителей персональных данных возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

6.3. Мероприятия по обеспечению целостности

6.3.1. Требования

Сохранность и целостность программных средств ИСПДн и персональных данных являются обязательными и обеспечиваются в том числе за счет создания резервных копий. Резервному копированию подлежат все программные средства, архивы, журналы, информационные ресурсы (данные), используемые и создаваемые в процессе эксплуатации ИСПДн.

В Администрации должен быть определен и документально зафиксирован состав и назначение ПО, используемого в ИСПДн. Порядок внесения изменений в установленное ПО ИСПДн, включая контроль действий программистов в процессе модификации ПО, должен быть регламентирован.

Эталонные копии ПО должны быть учтены, доступ к ним должен быть регламентирован.

С целью недопущения изменения состава ПО ИСПДн, из него должны быть исключены программные средства, предназначенные для разработки и отладки ПО (либо содержащие средства разработки, отладки и тестирования программно-аппаратного обеспечения).

Средства восстановления функций обеспечения безопасности персональных данных в ИСПДн должны предусматривать ведение не менее двух независимых копий программных средств.

В Администрации должны быть реализованы механизмы восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним и/или возникновения форс-мажорных ситуаций или воздействия опасных факторов окружающей среды.

Требования к периодичности осуществления резервного копирования и требования к носителям, предназначенным для записи на них резервных копий, определены в документе «Порядок проведения резервного копирования персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

6.3.2. Порядок проведения мероприятий

Порядок организации резервного копирования и восстановления массивов информации в Администрации определен в документе «Порядок проведения резервного копирования ПДн в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

Ответственность за организацию своевременного резервного копирования и восстановления информации, а также за надлежащее хранение резервных носителей, содержащих резервные копии данных, возлагается на должностное лицо ответственное за защиту ПДн.

6.4. Мероприятия по обеспечению антивирусной защиты

6.4.1. Требования

Для предотвращения возможности внедрения в ИСПДн вредоносного программного обеспечения в Администрации должны применяться антивирусные средства:

Требования к настройке антивирусных средств защиты определены в проектной документации на СЗПДн, процедуры по управлению антивирусными средствами определены в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности).

6.4.2. Порядок проведения мероприятий

Порядок использования антивирусных средств защиты определен в эксплуатационной документации на СЗПДн (Руководство администратора информационной безопасности).

Системный администратор Администрации, осуществляет:

- установку антивирусных средств защиты в соответствии с эксплуатационной и технической документацией к ним;
- настройку параметров антивирусных средств защиты согласно требованиям по обеспечению безопасности, определенным в проектной документации на СЗПДн;
- контроль эффективности работы антивирусных средств защиты;

Контроль соблюдения условий использования антивирусных средств защиты, предусмотренных эксплуатационной и технической документацией возлагается на должностное лицо ответственное за защиту ПДн.

6.5. Мероприятия по обеспечению криптографической защиты

6.5.1. Требования

В Администрации должны применяться следующие типы средств криптографической защиты информации, сертифицированные ФСБ России:

- СКЗИ для обеспечения безопасности ПДн, передаваемых по каналам связи между Администрацией и ИС сторонних организаций;
- средства электронной подписи, т.е. шифровальные (криптографические) средства, используемые для подписания передаваемых документов и проверки электронной подписи получаемых документов.

СКЗИ, применяемые в Администрации для защиты ПДн, должны иметь класс, определенный в Частной модели угроз безопасности ПДн при их обработке в ИСПДн Администрации. Частная модель угроз безопасности ПДн составляется на каждую ИСПДн.

Правила использования СКЗИ при обмене информацией со структурными подразделениями Администрации Ленинградской области должны быть определены в соответствующих регламентах, утвержденных уполномоченными должностными лицами Администрацией Ленинградской области.

Правила использования СКЗИ при обмене информацией со сторонними организациями СКЗИ должны быть определены условиями заключаемых договоров между Администрации и данными организациями.

В Администрации ведется учет всех применяемых СКЗИ, эксплуатационной и технической документации к ним, а также учет лиц, допущенных к работе с СКЗИ, предназначенными для обеспечения безопасности ПДн.

Требования к эксплуатации и учету применяемых в Администрации СКЗИ определены в документе «Порядок эксплуатации СКЗИ в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

6.5.2. Порядок проведения мероприятий

Порядок организации криптографической защиты в Администрации, определен в документе «Порядок эксплуатации СКЗИ в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

На должностное лицо, ответственное за выполнение работ по защите ПДн в Администрации, возлагается ответственность за обеспечение функционирования и безопасности СКЗИ согласно требованиям руководящих документов ФСБ России.

6.6. Мероприятия по обеспечению физической защиты

6.6.1. Основные требования по обеспечению физической защиты:

В целях предотвращения несанкционированного входа (вскрытия) в помещения, а также исключения возможности неконтролируемого проникновения в эти помещения посторонних лиц, в Администрации организуется и обеспечивается физическая охрана и техническая защита

помещений Администрации, с использованием охранной сигнализации, обеспечивающие сохранность технических средств обработки персональных данных, носителей персональных данных и средств защиты информации.

Защите подлежат следующие типы помещений:

- помещения, в которых осуществляется непосредственно обработка ПДн пользователями ИСПДн Администрации;
- серверные помещения, в которых установлено серверное, сетевое оборудование и технические средства защиты информации;
- архивные помещения, в которых организовано хранение бумажных документов, содержащих ПДн.

Перечень лиц, которые допускаются в указанные помещения, определяется распоряжением администрации.

В целях обеспечения физической защиты помещений применяться следующие средства защиты и контроля за несанкционированным вскрытием:

- система охранной сигнализации;
- двери помещений оборудуются замками для защиты от несанкционированного проникновения и местами для их опечатывания и сдачи под охрану.
- устанавливаются металлические двери для защиты от несанкционированного проникновения в серверные и архивные помещения.

В целях организации противопожарной безопасности в Администрации устанавливается система пожарной сигнализации

6.6.2. Порядок проведения мероприятий по обеспечению физической защиты:

Контроль обеспечения безопасности помещений, в которых расположены компоненты ИСПДн, возлагается на должностное лицо ответственное за защиту ПДн.

Доступ в защищаемые помещения осуществляется согласно перечню утвержденного распоряжением администрации.

Лица, не указанные в Перечне допущенных в защищаемые помещения, при наличии необходимости могут посещать помещения Администрации только в сопровождении допущенных лиц.

Одиночное, бесконтрольное пребывание лиц, не допущенных к работе по обработке ПДн, в производственных помещениях - **СТРОГО ЗАПРЕЩЕНО**.

Пребывание посторонних лиц в серверных помещениях допускается в целях производственной необходимости, только в присутствии должностного лица, ответственного за защиту ПДн.

В случае утраты ключей (либо подозрении на утрату) к замкам в защищаемые помещения предпринимаются следующие меры:

- оповещаются должностные лица, ответственные за организацию работ по обработке ПДн за защиту ПДн служебной запиской;
- производится немедленная замена запираемых замков.
- назначается административная проверка всех режимных помещений с составлением акта и принятым мерам, виновные лица привлекаются к административной ответственности.

При возникновении форс-мажорных обстоятельств в защищаемых помещениях (возникновение пожара, затопление помещения, возгорание электропроводки и прочее) в отсутствии лиц, имеющих доступ в эти помещения, осуществляется вскрытие помещений с соблюдением следующих условий:

- оповещаются должностные лица ответственные за организацию работ по обработке и защите ПДн;
- помещения вскрываются группой в составе не менее двух человек;
- при вскрытии помещения составляется акт о вскрытии, в котором указываются должности и фамилии лиц, вскрывших помещение, дата, время и причины вскрытия.

7. Обязанности, права и ответственность должностных лиц при обеспечении безопасности ПДн

Обязанности, права и ответственность должностных лиц, участвующих в обеспечении безопасности ПДн в Администрации определены в соответствующих инструкциях.

8. Планирование работ по защите ПДн

Планирование работ по защите информации, требования к содержанию плана, порядок разработки, согласования, утверждения и оформления плана, порядок отчетности и контроля над его выполнением определяются действующими нормативными документами РФ.

План определяет перечень основных проводимых организационно-технических мероприятий по защите информации (в том числе ПДн) в Администрации с указанием:

- сроков выполнения мероприятий;
- ответственных за выполнение соответствующих пунктов Плана работников.

В План включаются:

- мероприятия по контролю состояния защищенности ПДн;

План на очередной календарный год разрабатывается должностным лицом, ответственным за защиту информации в ИС ПДн, который осуществляет общий контроль над выполнением работ по защите информации.

Утвержденный план хранится у должностного лица ответственного за организацию работ по обработке ПДн.

Отчет о результатах выполнения запланированных мероприятий по обеспечению безопасности ПДнза текущий год формируется должностным лицом, ответственным за защиту ПДн, в рамках общего отчета работы за текущей год.

9. Контроль состояния защищенности ПДн

Контроль состояния защищенности ПДн в Администрации осуществляется с целью своевременного выявления и предотвращения утечки конфиденциальной информации, отнесенной к категории ПДн, вследствие НСД к ней, преднамеренных программно-технических воздействий на персональные данные и оценки защищенности ПДн (далее по тексту - Контроль).

Контроль заключается в проверке выполнения требований действующих нормативных документов в области обработки и обеспечения безопасности ПДн, в оценке обоснованности и эффективности принятых мер по защите ПДн.

Контроль эффективности внедренных мер и СЗИ, входящих в состав СЗПДн, должен проводиться в соответствии с требованиями эксплуатационной документации на СЗПДн в целом на конкретные СЗИ, а также требованиями других нормативных документов не реже одного раза в год.

Обязательным является контроль СЗИ, входящих в состав СЗПДн, при вводе их в эксплуатацию после проведения ремонта таких средств, а также при изменении условий и расположения их эксплуатации.

Контроль обеспечения безопасности ПДн в Администрации организовывается должностным лицом, ответственным за проведение работ по защите ПДн в Администрации.

Контроль состояния и эффективности СЗПДн может осуществляться в соответствии с планом основных мероприятий по защите информации на текущий год или носить внеплановый характер.

Результаты периодического контроля оформляются отдельными протоколами или актами.

По всем выявленным нарушениям требований по защите ПДн должностное лицо, ответственное за обеспечение безопасности ПДн в Администрации, в пределах предоставленных ему прав и своих функциональных обязанностей обязано добиваться их немедленного устранения.

Должностное лицо, ответственное за организацию работ по обработке ПДн в Администрации, обязано принять все необходимые меры по немедленному устранению выявленных нарушений. При невозможности их немедленного устранения должна быть прекращена обработка ПДн и организованы работы по устранению выявленных нарушений.

Работники Администрации, осуществляющие обработку ПДн в ИСПДн, обязаны выполнять требования должностного лица ответственного за обеспечение безопасности ПДн, по устранению допущенных ими нарушений норм и требований по обработке и/или обеспечении безопасности ПДн. Также работники несут персональную ответственность за соблюдение требований по обеспечению безопасности ПДн в ходе проведения работ.

Учет, хранение и выдача работникам паролей и ключей для системы защиты ПДн от НСД, оперативный контроль действий работников, осуществляющих обработку ПДн, осуществляет должностное лицо ответственное за обеспечение безопасности ПДн.

10. Управление инцидентами информационной безопасности

В Администрации в целях своевременного устранения выявленных нарушений безопасности определен и задокументирован порядок действий при возникновении инцидентов информационной безопасности, связанных с нарушением требований по обработке и обеспечению безопасности ПДн.

10.1. Требования к мероприятиям

К инцидентам информационной безопасности, связанным с нарушением требований по обработке и обеспечению безопасности ПДн, относятся любые нарушения, приводящие к снижению уровня защищенности ИСПДн, в том числе несоблюдение условий хранения носителей ПДн и использования средств защиты информации, которые могут привести к нарушению конфиденциальности, целостности или доступности ПДн.

В Администрациив случаях возникновения подобных инцидентов информационной безопасности проводятся разбирательства, составляются заключения по фактам возникновения инцидентов, разрабатываются и принимаются меры по предотвращению возможных последствий инцидентов.

10.2. Порядок проведения мероприятий

Организация и контроль процесса реагирования на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн, в Администрации возлагается на должностное лицо ответственное за обеспечение безопасности ПДн.

Процедура управления инцидентами информационной безопасности, связанными с нарушением требований по обработке и обеспечению безопасности ПДн, регламентирована в документе «Порядок реагирования на инциденты информационной безопасности в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области». Данный документ определяет порядок проведения следующих мероприятий:

- определение инцидента информационной безопасности;
- оповещение ответственного лица о возникновении инцидента;
- устранение последствий и причин инцидента;
- расследование инцидента;
- реализация необходимых корректирующих и превентивных мер.

Дополнительно порядок действий работников Администрации в случаях возникновения инцидентов информационной безопасности определен в документе «Инструкция пользователю информационной системы ПДн в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области».

11. Модернизация системы защиты ПДн

Для определения необходимости модернизации СЗПДн не реже одного раза в год должностным лицом ответственным за обеспечение безопасности

ПДн проводится проверка состава и структуры СЗПДн, состава угроз и уровня защищенности ПДн, обработка которых осуществляется в ИСПДн Администрации.

Модернизация СЗПДн в обязательном порядке проводится в случаях, если:

- изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав обрабатываемых ПДн, состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и пр.);
- изменился состав угроз безопасности ПДн в ИСПДн;
- изменился уровень защищенности ПДн.

Выбор мер и СЗИ, входящих в состав СЗПДн, проводится на основании проведенного анализа угроз и проведенной классификации ИСПДн (определения уровня защищенности ПДн). Порядок проведения данных мероприятий определен в Разделах 5.1.4 «Определение угроз безопасности данных» и 5.1.5 «Определение уровня защищенности ПДн» настоящего Положения.

Должностное лицо ответственное за обеспечение безопасности ПДн ежегодно разрабатывает план работ по обеспечению безопасности ПДн в Администрации, в котором определяется перечень необходимых мероприятий по обеспечению безопасности ПДн с учетом уже выполненных мероприятий.

В план работ по обеспечению безопасности ПДн включаются организационные и технические мероприятия, направленные на выполнение требований нормативно-правовых документов в области безопасности ПДн и на совершенствование СЗПДн, а также контрольные мероприятия и мероприятия по проведению обучения работников Администрации. В плане указываются дата, сроки проведения мероприятий, их периодичность (разовые или регулярные) и назначаются ответственные за их организацию и выполнение лица.

Работники, участвующие в обеспечении безопасности ПДн в Администрации вправе формировать предложения по совершенствованию СЗПДн и направлять их на рассмотрение должностному лицу ответственному за защиту ПДн, которое в свою очередь формирует сводный перечень предложений по совершенствованию СЗПДн.

Ежегодно должностное лицо ответственное за защиту ПДн формирует отчет о проделанных мероприятиях по выполнению плана работ по обеспечению безопасности ПДн, обрабатываемых в Администрации, и предоставляет его главе администрации совместно со сводным перечнем предложений по совершенствованию СЗПДн.

Ежегодный отчет по выполнению плана работ включает в себя:

- результаты проведенной проверки состава и структуры, состава угроз и уровня защищенности ПДн;
- результаты проведенных контрольных мероприятий по защите ПДн;
- результаты проверок регулирующими органами;
- результаты анализа инцидентов информационной безопасности;
- результаты плановых мероприятий по обеспечению безопасности ПДн;
- предложения по совершенствованию СЗПДн на основе полученных результатов.

На основании решения, принятого главой администрации, по результатам рассмотрения ежегодного отчета и предложений по совершенствованию СЗПДн должностное лицо ответственное за защиту ПДн составляет план работ по обеспечению безопасности ПДн, обрабатываемых в администрации, на следующий год.

12. Привлечение сторонних организаций для проведения мероприятий по обеспечению безопасности ПДн

В Администрации могут привлекаться сторонние организации для проведения следующих мероприятий по обеспечению безопасности ПДн:

- разработка нормативно-методических материалов по вопросам обеспечения безопасности ПДн;
- поставка СЗИ и СКЗИ;

- выполнение организационных и технических мероприятий в области защиты ПДн, на проведение которых у Администрации отсутствует соответствующее разрешение либо отсутствуют технические средства и подготовленные работники (специалисты);

- выполнение организационных и технических мероприятий в области защиты ПДн, выполнение которых силами Администрации экономически нецелесообразно;

- подтверждение соответствия мер по защите ИСПДн требованиям нормативно-правовой базы РФ в области безопасности ПДн, путем проведения аттестационных испытаний ИСПДн Администрации по требованиям безопасности информации;

- контроль и аудит эффективности проводимых мероприятий по защите ПДн.

Привлекаемые для оказания услуг в области защиты ПДн сторонние организации должны иметь лицензии на соответствующие виды деятельности.

Перечень совместно выполняемых организационных и технических мероприятий в области защиты ПДн определяется с учетом планируемых работ по созданию (реконструкции) ИСПДн и включается в План основных мероприятий по защите ПДн.

В данном разделе определен порядок взаимодействия с вышеперечисленными сторонними организациями.

12.1. Привлечение сторонних организаций для проведения мероприятий по созданию и модернизации СЗПДн и/или проведению контрольных мероприятий

Привлекаемая сторонняя организация должна обладать соответствующими, проводимым работам, лицензиями и сертификатами.

Должностное лицо, ответственное за обеспечение безопасности ПДн, является ответственным за выбор организации, привлекаемой для проведения мероприятий по созданию или модернизации СЗПДн и проведению контрольных мероприятий. Должностное лицо, ответственное за защиту ПДн, осуществляет подбор подходящих организаций и формирует предложения для согласования с главой администрации.

Существенным условием договора является обязательство привлекаемой организации обеспечить конфиденциальность получаемой информации, ставшей известной в ходе выполнения работ по обеспечению безопасности ПДн в администрации.

В случае привлечения сторонней организации для проведения мероприятий по созданию или модернизации СЗПДн в договоре прописываются обязательства привлекаемой организации по проведению необходимых организационно-технических мероприятий, включающих в себя:

- организацию и проведение работ по созданию СЗПДн;

- реализацию требований нормативно-правовых документов РФ в области обработки и защиты ПДн;

- своевременное совершенствование СЗПДн;

- поддержание работоспособности и сопровождение СЗПДн.

В случае привлечения сторонней организации для проведения контрольных мероприятий (аудит обеспечения безопасности ПДн) в договоре прописываются обязанности привлекаемой организации по выполнению необходимых работ, включающих в себя:

- проверку выполнения требований нормативно-правовых документов РФ в области обработки и защиты ПДн;

- оценку обоснованности и эффективности принятых в Администрации мер по обеспечению безопасности ПДн.

Должностное лицо, ответственное за обеспечение безопасности ПДн, осуществляет контроль над выполнением привлекаемой организацией взятых на себя обязательств.

12.2. Привлечение сторонних организаций для проведения обучения работников

К организациям, привлекаемым для проведения обучения работников Администрации по направлению обеспечения безопасности ПДн, предъявляются следующие требования:

- организация должна иметь лицензию на осуществление образовательной деятельности, выданную Министерством образования РФ, государственными органами управления образованием субъектов РФ или органами местного самоуправления, наделенными соответствующими полномочиями;
- предлагаемые организацией программы и курсы обучения должны быть согласованы с регулирующими и надзорными органами;
- по результатам проведенного обучения организация должна проводить итоговую аттестацию работников.

12.3. Привлечение сторонних организаций (подрядчиков) для ремонтно-восстановительных работ

Организацией обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн, в Администрации занимается системный администратор Администрации. В случае необходимости, ремонт технических средств может быть произведен с привлечением специалистов сторонних организаций на договорной основе с составлением актов выполненных работ.

Должностным лицом, ответственным за обеспечение безопасности ПДн, определяется порядок привлечения сторонних организаций (подрядчиков) для обслуживания, настройки и ремонта средств обработки и СЗИ, входящих в состав СЗПДн.

Сопровождение и контроль сторонних организаций (подрядчиков) обеспечивается должностным лицом, ответственным за обеспечение безопасности ПДн.

Обязательным условием при передаче технических средств обработки ПДн и машинных носителей ПДн для осуществления ремонтных работ сторонней организацией является удаление ПДн с носителей, установленных на передаваемых устройствах, либо извлечение носителей ПДн. Контроль исполнения данного требования возлагается на должностное лицо ответственное за защиту ПДн. В случае, когда выполнить данное требование не представляется возможным, должностным лицом, ответственным за защиту ПДн, составляется двусторонний протокол, в котором указано, что сторонняя организация осведомлена о том, какие именно персональные данные содержатся на носителе и обязана принять все необходимые меры по обеспечению их безопасности.

После проведения ремонта средств защиты или средств обработки ПДн, при изменении условий их расположения или эксплуатации обязательно осуществляется проверка готовности этих средств к использованию с составлением заключений о возможности их эксплуатации.

13. Пересмотр и внесение изменений

Настоящее Положение должно пересматриваться в случаях:

- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;
- изменением организационной и технологической инфраструктуры, в рамках которой обрабатываются ПДн;
- выявления снижения общего уровня информационной безопасности (по результатам регулярного мониторинга или аудита);

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за обеспечение безопасности ПДн в Администрации.

Внесение изменений производится на основании соответствующего распоряжения Администрации.

Приложение № 3

УТВЕРЖДЕНО
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПРАВИЛА
работы с обезличенными персональными данными
в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

Статья 1. Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса используемых информационных систем персональных данных и по достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством Российской Федерации.

Статья 2. Способы обезличивания

1. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:
1) замена части сведений идентификаторами;
2) обобщение (понижение) точности некоторых сведений;
3) деление сведений на части и обработка их в разных информационных системах;
4) другие способы.
2. К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

Статья 3. Правила работы с обезличенными данными

1. Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.
2. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.
3. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:
1) использование средств защиты информации;
2) использование антивирусных программ;
3) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных;
4. При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:
1) хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;
2) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

Приложение № 4

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в связи с реализацией трудовых отношений, а также в связи с оказанием государственных или муниципальных услуг и осуществлением государственных или муниципальных функций

Перечень персональных данных, обрабатываемых в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в связи с реализацией трудовых отношений:

1) Фамилия, имя, отчество;
2) Место, год и дата рождения;
3) Адрес регистрации;
4) Адрес проживания (реальный);
5) Телефонный номер (домашний, рабочий, мобильный);
6) адрес электронной почты;
7) Паспортные данные (серия, номер, кем и когда выдан);
8) Семейное положение и состав семьи (муж/жена, дети);
9) Места рождения, работы, домашние адреса близких родственников;
10) Оклад и другие доходы;
11) индивидуальный номер налогоплательщика;
12) Номер пенсионного страхования;
13) Данные о трудовом договоре (№ трудового договора, дата его заключения, дата начала и дата окончания договора, вид работы, срок действия договора, наличие испытательного срока, режим труда, длительность основного отпуска, длительность дополнительного отпуска, длительность дополнительного отпуска за ненормированный рабочий день, обязанности работника, дополнительные социальные льготы и гарантии, № и число изменения к трудовому договору, характер работы, форма оплаты, категория персонала, условия труда, продолжительность рабочей недели, система оплаты);
14) Информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающие образование: наименование, номер, дата выдачи, специальность);
15) Информация о трудовой деятельности до приема на работу;
16) Информация о знании иностранных языков;
17) Сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
18) Данные о медицинской страховке;
19) Данные об аттестации работников;
20) Данные о повышении квалификации;
21) Данные о наградах, медалях, поощрениях, почетных званиях;
22) Информация о состоянии здоровья;
23) Информация о негосударственном пенсионном обеспечении;
24) Данные об имущественном и социальном положении;
25) Сведения о доходах, имуществе и обязательствах имущественного характера, а также о доходах, об имуществе и обязательствах имущественного характера членов семьи;
26) Сведения о социальных льготах и социальном статусе;
27) Сведения о наличии (отсутствии) судимости;

28) Номера расчетных счетов, банковских карт;
29) Сведения о допуске к государственной тайне;
30) Сведения о пребывание за границей.

Перечень персональных данных, обрабатываемых в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в связи с оказанием муниципальных услуг и осуществлением муниципальных функций:

1) Фамилия, Имя, Отчество;
2) Дата рождения;
3) Адрес регистрации (адрес проживания);
4) Паспортные данные (серия, номер, кем и когда выдан);
5) Семейное положение и состав семьи (муж/жена, дети);
6) Оклад и другие доходы;
7) номера контактных телефонов;
8) адрес электронной почты;
9) индивидуальный номер налогоплательщика;
10) Номер пенсионного страхования;
11) Имущественное положение;
12) Социальное положение;
13) Образование;
14) Место работы;
15) Причина и место смерти (серия, номер, кем выдано свидетельство о смерти, сведения об актовой записи).

Обезличенные и (или) общедоступные персональные данные:
-сведения о трудовой деятельности (общие данные о трудовой занятости на текущее время, общий и непрерывный стаж работы);
-сведения об образовании, квалификации, о наличии специальных знаний или специальной подготовки (дата начала и завершения обучения, факультет или отделение, квалификация и специальность по окончании образовательного учреждения, ученая степень, ученое звание, владение иностранными языками);
-сведения о повышении квалификации и переподготовке (дата начала и завершения обучения, квалификация и специальность по окончании образовательного учреждения);
-сведения о заработной плате (в том числе данные по окладу, надбавкам, налогам);
— сведения о воинском учете военнообязанных лиц и лиц, подлежащих призыву на военную службу (военно-учетная специальность, воинское звание, данные о принятии/снятии с учета);
-сведения о семейном положении (состоянии в браке, наличие детей и их возраст);
— наличие (отсутствие) судимости.

Приложение № 5

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПЕРЕЧЕНЬ
должностей в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных

- заместитель главы администрации
- начальник отдела

Приложение № 6

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПЕРЕЧЕНЬ

должностей в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

- глава муниципального образования;

- заместитель главы администрации;
- начальник отдела;
- главный специалист;
- ведущий специалист;
- специалист;
- администратор;
- инспектор ВУС.

Приложение № 7

УТВЕРЖДЕНА
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № _81

Форма обязательства
о неразглашении информации, содержащей персональные данные

Я, _____
(фамилия, имя, отчество лица, допущенного к обработке персональных данных)
_____,
исполняющий(ая) должностные обязанности _____
_____
_____,
предупрежден(а) о том, что на период исполнения должностных обязанностей мне будет предоставлен допуск к информации, содержащей персональные данные.

Настоящим добровольно принимаю на себя обязательства:

1. Не передавать и не разглашать третьим лицам информацию, содержащую персональные данные, которая мне доверена (будет доверена) или станет известной в связи с исполнением должностных обязанностей.
2. В случае попытки третьих лиц получить от меня информацию, содержащую персональные данные, сообщать непосредственному начальнику.
3. Не использовать информацию, содержащую персональные данные, с целью получения выгоды.
4. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты персональных данных.
5. В случае расторжения договора (контракта) и (или) прекращения права на допуск к информации, содержащей персональные данные, не разглашать и не передавать третьим лицам известную мне информацию, содержащую персональные данные.

Я предупрежден(а) о том, что нарушение данного обязательства является основанием привлечения к дисциплинарной и(или) иной ответственности в соответствии с законодательством Российской Федерации.

«____» _____ 20 г _____/_____
(подпись) (расшифровка подписи)

Приложение № 8

УТВЕРЖДЕНО
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81_____

Согласие на обработку персональных данных

_____
(Наименование (Ф.И.О.) оператора, получающего согласие субъекта персональных данных)

_____
(Адрес оператора)

_____
(Ф.И.О. субъекта персональных данных)

_____
(Адрес, где зарегистрирован субъект персональных данных)

_____
(Номер основного документа, удостоверяющего его личность, сведения о дате выдачи документа и выдавшем его органе)

Даю своё согласие на обработку следующих персональных данных:

_____
(Перечень персональных данных)

с целью:_____
(Указывается цель обработки персональных данных)

Даю своё согласие на совершение следующих действий с моими персональными данными (**ненужное зачеркнуть**): сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Даю своё согласие на использование следующих способов обработки моих персональных данных (**ненужное зачеркнуть**):

- с использованием средств автоматизации (автоматизированная обработка);
- без использования средств автоматизации (неавтоматизированная обработка);
- смешанная обработка.

Срок, в течение которого действует согласие: _____
(Указывается срок действия согласия)

В случае неправомерных действий или бездействия оператора настоящее согласие может быть отозвано мной заявлением в письменном виде.

Дата:_____ _____ _____
(подпись) (инициалы, фамилия)

Приложение № 9

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПОРЯДОК

доступа в помещения, в которых ведётся обработка персональных данных, в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

1. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении, в котором осуществляется обработка персональных данных.

2. Все сотрудники, постоянно работающие в помещениях, в которых ведётся обработка персональных данных, должны быть допущены к работе с соответствующими видами персональных данных.

3. В служебных помещениях применяются технические и организационные меры, направленные для защиты данных от нецелевого использования, несанкционированного доступа, раскрытия, потери, изменения и уничтожения обрабатываемых персональных данных.

К указанным мерам относятся:

1) технические меры защиты: применение антивирусных программ, программ защиты, установление паролей на персональных компьютерах;

2) организационные меры защиты: обучение и ознакомление с принципами безопасности и конфиденциальности, доведение до операторов обработки персональных данных важности защиты персональных данных и способов обеспечения защиты.

Приложение № 10

УТВЕРЖДЕНЫ
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПРАВИЛА

рассмотрения запросов субъектов персональных данных или их представителей в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

Статья 1. Право субъектов персональных данных на получение сведений

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных оператором;

2) правовые основания и цели обработки персональных данных;

3) цели и применяемые оператором способы обработки персональных данных;

4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) порядок осуществления субъектом персональных данных прав, предусмотренных настоящим Федеральным законом;

8) информацию об осуществленной или о предполагаемой трансграничной передаче данных;

9) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

10) иные сведения, предусмотренные настоящим Федеральным законом или другими федеральными законами.

Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе если:

1) обработка персональных данных, включая персональные данные, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

2) обработка персональных данных осуществляется органами, осуществившими задержание субъекта персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинение по уголовному делу, либо применившими к субъекту персональных данных меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;

3) обработка персональных данных осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

4) доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц;

5) обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

2. Субъект персональных данных имеет право требовать от оператора уточнения его персональных данных, их блокирования или уничтожения, в случае если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Статья 2. Порядок предоставления оператором сведений по запросу субъекта персональных данных

1. При обращении либо при получении запроса субъекта персональных данных или его представителя сведения должны быть предоставлены в

доступной форме. Запрос регистрируется в день поступления в установленном порядке.

2. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с оператором (номер договора, дата заключения, условное словесное обозначение и (или) иные сведения), либо сведения , иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его представителя.

3. Оператор при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных, обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными в течении 30 (тридцати) дней с даты получения запроса.

В случае отказа в предоставлении информации о наличии персональных данных оператор обязан дать в письменной форме мотивированный ответ с ссылкой на действующее законодательство, являющегося основанием для такого отказа. Отказ в предоставлении информации направляется в срок, не превышающий 30 (тридцати) дней со дня получения запроса субъекта персональных данных.

4. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор в срок, не превышающий 7 (семь) рабочих дней, вносит в них необходимые изменения. О внесённых изменениях уведомляется субъект персональных данных или его представитель.

5. В случае предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные в срок, не превышающий 7 (семь) рабочих дней. Об уничтоженных персональных данных уведомляется субъект персональных данных или его представитель.

6. При получении запроса из уполномоченного органа по защите прав субъектов персональных данных оператор обязан сообщить необходимую информацию в течении 30 (тридцати) дней с даты получения такого запроса.

7. Возможность ознакомления с персональными данными предоставляется на безвозмездной основе лицом ответственным за обработку персональных данных.

Приложение № 11

УТВЕРЖДЕНЫ
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Статья 1. Цель внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных осуществляется с целью проверки соответствия обработки персональных данных требованиям к защите персональных данных, установленных Федеральным законом №152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

Статья 2. Виды и периодичность внутреннего контроля.

1. Внутренний контроль соответствия обработки персональных данных делится на текущий и периодический.
2. Текущий внутренний контроль осуществляется на постоянной основе Ответственным за обеспечение безопасности персональных данных.
3. Периодический внутренний контроль осуществляется комиссией в соответствии с поручением главы муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

Периодичность проверки – **не реже одного раза в шесть месяцев**.

Статья 3. Порядок создания комиссии для осуществления внутреннего контроля.

1. Проверки осуществляются комиссией, созданной распоряжением главы администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области, из числа сотрудников администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области, допущенных к обработке персональных данных, так же возможно привлечение в качестве членов комиссий экспертов.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

2. Проверки осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра рабочих мест сотрудников, участвующих в процессе обработки персональных данных.

Статья 4. Порядок проведения внутренней проверки.

1. При проведении внутренней проверки комиссией должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности персональных данных;

- состояние учёта бумажных и машинных носителей персональных данных;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным;
- мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- осуществление мероприятий по обеспечению целостности персональных данных.

2. Осуществлении внутреннего контроля мероприятий проводятся комиссией периодически в соответствии с Перечнем мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных. Форма Перечня мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных приведена в Приложении 1 к настоящим Правилам.

Для каждой проверки составляется Протокол проведения внутренней проверки. Форма Протокола приведена в Приложении 2 к настоящим Правилам.

3. При выявлении в ходе проверки нарушений в Протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

4. Протоколы хранятся у председателя комиссии в течение текущего года. Уничтожение Протоколов проводится комиссией самостоятельно по истечении срока хранения.

5. О результатах проверки и мерах, необходимых для устранения нарушений председатель комиссии докладывает главе муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

6. Срок проведения проверки не может составлять более 30 (тридцати) дней со дня принятия решения о её проведении.

Приложение 1

Перечень

мероприятий для осуществления внутреннего контроля за выполнением требований к защите персональных данных при их обработке в информационных системах персональных данных

№ п/п	Краткое описание мероприятий
1	Контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны
2	Проверка выполнения требований по условиям размещения автоматизированных рабочих мест (далее - АРМ) в помещениях, в которых размещены средства информационных систем персональных данных (далее - ИСПДн)
3	Проверка соответствия состава и структуры программно-технических средств ИСПДн документированному составу и структуре средств, разрешенных для обработки персональных данных
4	Проверка режима допуска в помещения, где размещены средства ИСПДн и осуществляется обработка персональных данных
5	Проверка соответствия реального уровня полномочий по доступу к персональным данным различных пользователей, установленному в списке лиц, допущенных к обработке персональных данных, уровню полномочий
6	Проверка наличия и соответствия средств защиты информации в соответствии с указанными в техническом паспорте на ИСПДн
7	Проверка правильности применения средств защиты информации
8	Проверка неизменности настроенных параметров антивирусной защиты на рабочих станциях пользователей
9	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн
10	Проверка соблюдения правил парольной защиты
11	Проверка работоспособности системы резервного копирования
12	Проведение мероприятий по проверке организации учета и условий хранения съемных носителей персональных данных
13	Проверка соблюдения требований по обеспечению безопасности при использовании ресурсов сети "Интернет"
14	Проверка знаний работниками руководящих документов, технологических инструкций, предписаний, актов, заключений и уровня овладения работниками технологией безопасной обработки информации, изложенных в инструкциях
15	Проверка знаний инструкций по обеспечению безопасности информации пользователями ИСПДн
16	Проверка наличия документов, подтверждающих возможность применения технических и программных средств вычислительной техники для обработки персональных данных и применения средств защиты (сертификатов соответствия и других документов)

Приложение 2

Протокол
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

Настоящий Протокол составлен в том, что __.__.202_ комиссией по внутреннему контролю проведена проверка _____
_____.
место проверки

Проверка осуществлялась в соответствии с требованиями _____
_____
_____
название документа

В ходе проверки проверено:
_____
_____
_____
_____
_____

Выявленные нарушения:
_____
_____
_____
_____
_____
_____

Меры по устранению нарушений:
_____
_____
_____
_____
_____
_____

Срок устранения нарушений: _____.

Председатель комиссии _____ И.О. Фамилия

Члены комиссии:
Должность _____ И.О. Фамилия
Должность _____ И.О. Фамилия

Должность руководителя
проверяемого подразделения _____ И.О. Фамилия

Приложение № 12

УТВЕРЖДЕНА
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ИНСТРУКЦИЯ

по организации антивирусной защиты в информационных системах персональных данных администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

1. Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты в информационных системах персональных данных (далее –ИСПДн) и устанавливает ответственность за их выполнение.

2. Основные определения

Вредоносное программное обеспечение (далее ПО) - специально разработанное программное обеспечение, программный модуль, блок, группа команд, имеющая способность к самораспространению, которая может попадать в общее и специальное программное обеспечение ИСПДн и приводить к:

- дезорганизации вычислительного процесса (нарушению или существенному замедлению обработки информации);
- модификации или уничтожению программ, или данных;
- приведению в негодность носителей информации и других технических средств;
- нарушению функционирования средств защиты информации.

3. Инструкция по применению средств антивирусной защиты

Защита ПО ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.

1.1. К использованию допускаются только лицензионные антивирусные средства, обладающие необходимой сертификацией в регулирующих органах РФ.

1.2. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на системного администратора Администрации.

1.3. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.

1.4. Всё впервые вводимое в эксплуатацию ПО должно проходить обязательный антивирусный контроль.

1.5. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места системного администратора Администрации.

1.6. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах ИСПДн.

1.7. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов ИСПДн.

1.8. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.

1.9. Контроль входящей информации необходимо проводить непосредственно после ее приема.

1.10. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.

1.11. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

1.12. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к системному администратору Администрации.

1.13. При получении информации о возникновении вирусной эпидемии вне ИС должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.

1.14. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса системного администратора Администрации;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к администратору безопасности ИСПДн.

1.15. По факту обнаружения зараженных вирусом файлов системный администратор Администрации должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

1.16. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.

1.17. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

1.18. Ответственный за организацию обработки ПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.

1.19. С данной инструкцией Пользователи должны быть ознакомлены под роспись в листе ознакомления с данной инструкцией.

1.20. Проводить периодическое тестирование функций средств антивирусной защиты.

1.21. Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).

Приложение № 13

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПОРЯДОК

учета, хранения и уничтожения носителей персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

1. Термины и определения

В настоящем Порядке использованы следующие термины и определения:

Информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Конфиденциальная информация: Информация, доступ к которой ограничивается в соответствии с действующим законодательством РФ, и иными регламентирующими документами.

Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

Обработка персональных данных: Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Персональные данные: Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь персональных данных: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных: Процесс, в котором присутствует обработка персональных данных.

Уничтожение персональных данных: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	Описание
1.	**ИСПДн**	Информационная система персональных

		данных
2.	**ОС**	Операционная система
3.	**ПДн**	Персональные данные
4.	**СВТ**	Средство вычислительной техники
5.	**СЗПДн**	Система защиты персональных данных

3. Область применения

Настоящий Порядок учета, хранения и уничтожения носителей ПДн (далее - Порядок) предназначен для определения единого порядка обращения с машинными (электронными) и бумажными носителями персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области (далее - Администрация).

4. Общие положения

Настоящий Порядок устанавливает порядок учета, хранения, использования и уничтожения носителей ПДн в процессах обработки ПДн.

Настоящий Порядок разработан в соответствии с документом «Положение об обеспечении безопасности персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

5. Порядок работы с бумажными носителями

5.1. Порядок учета бумажных носителей, содержащих ПДн

Любой документ, содержащий ПДн, является конфиденциальным и подлежит обязательному учету. Учет документов, содержащих ПДн, осуществляется в соответствии с положениями настоящего Порядка.

Ответственность за организацию ведения учета документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

5.2. Порядок хранения бумажных носителей, содержащих ПДн

С целью обеспечения физической сохранности документов, содержащих ПДн, предотвращения хищения документов, а также с целью недопущения разглашения содержащихся в них сведений документы должны храниться в местах, исключающих доступ к ним посторонних лиц.

Хранение открытых документов вместе с конфиденциальными документами разрешено только в случаях, когда они являются приложениями к конфиденциальным документам.

Рабочее место работника Администрация должно быть организовано таким образом, чтобы исключить возможность просмотра документов с ПДн лицами, которые не допущены к ПДн.

Во время работы на столе должны находиться только те документы, непосредственно с которыми ведется работа, все остальные должны быть убраны в места, предназначенные для хранения.

5.3. Порядок уничтожения бумажных носителей, содержащих ПДн

Основанием для уничтожения документов, содержащих ПДн, является достижение целей обработки.

Локальные документы, содержащие ПДн, уничтожаются по мере необходимости.

Ответственность за своевременное уничтожение документов возлагается на должностное лицо ответственное за организацию работ по обработке ПДн.

Уничтожение документов производится с помощью специальных бумагорезательных технических средств (шредеров) или сжиганием.

5.3.1. Уничтожение массивов документов

Массивы документов (архивы, библиотеки и т.п.) уничтожаются под контролем должностного лица ответственного за защиту ПДн.

Экспертиза документа проводится раз в год. Экспертиза охватывает все документы, содержащие ПДн, за соответствующий период времени.

Экспертиза проводится путем изучения содержания документов. Цель проведения экспертизы - определить возможность уничтожения документов либо дальнейшие сроки их хранения.

После проведения экспертизы составляется Акт о выделении дел и документов, подлежащих уничтожению (Приложение А). В Акт включаются отобранные дела для уничтожения, отдельные документы из дел и документы выделенного хранения.

Уничтожение массивов документов производится с помощью бумагорезательных технических средств или сжиганием.

Если уничтожение массивов документов производит третья сторона, с которой заключен соответствующий договор, то документы, выделенные для уничтожения, помещаются в короба, после чего короба запечатываются передаются третьей стороне.

После уничтожения массива документов должностными лицами ответственными за организацию работ по обработке ПД и за защиту ПДн, а также работниками производившими уничтожение документов подписывается Акт об уничтожении документов, содержащих ПДн (Приложение Б).

6. Порядок работы с машинными носителями

Учету подлежат следующие типы машинных носителей ПДн:

- отчуждаемые носители информации (внешние жесткие магнитные диски, гибкие магнитные диски, магнитные ленты, USB флеш-накопители, карты флеш-памяти, оптические носители (CD, DVD и прочее);
- неотчуждаемые носители информации (жесткие магнитные диски).

6.1. Порядок учета машинных носителей, содержащих ПДн

Все отчуждаемые машинные носители данных, используемые при работе со средствами вычислительной техники (далее - СВТ) для обработки и хранения ПДн, обязательно регистрируются и учитываются в **Журнале учета выдачи машинных носителей ПДн (Приложение В)**.

Неотчуждаемые носители информации подлежат учету в составе системных блоков СВТ, которые в свою очередь учитываются в Техническом паспорте ИСПДн.

Ответственность за ведение Журнала учеты выдачи машинных носителей ПДн и контроль учета носителей ПДн возлагается на системного администратора Администрации.

Каждому машинному носителю, содержащему ПДн, присваивается учетный номер согласно Журналу.

В качестве учетного номера допускается использование серийного (заводского) номера носителя. В случае отсутствия серийного номера, учетный номер наносится на носитель информации или его корпус. Если невозможно маркировать непосредственно машинный носитель данных, то маркируется упаковка, в которой хранится носитель. В этом случае учетный номер записывается также на носитель машинным способом.

6.2. Порядок использования машинных носителей ПДн

Машинные носители ПДн выдаются пользователям или другим лицам, участвующим в обработке ПДн, для работы под подпись в Журнале. По завершении работы машинные носители ПДн сдаются обратно.

В случае повреждения машинных носителей ПДн, работник, за которым закреплен носитель, сообщает о случившемся должностному лицу ответственному за защиту ПДн.

Передача носителя, содержащего ПДн, третьим сторонам производится в соответствии с требованиями договора между Администрация и третьим

лицом.

Машинные носители ПДн пересылаются в том же порядке, что и документы.

При фиксации ПДн на машинных носителях не допускается фиксация на одном машинном носителе ПДн, цели обработки которых заведомо не совместимы.

Вынос машинных носителей, содержащих ПДн, за пределы контролируемой зоны Администрация запрещается без соответствующего разрешения должностного лица ответственного за защиту ПДн.

6.3. Порядок хранения машинных носителей ПДн

Хранение носителей, содержащих ПДн, осуществляется в условиях, исключающих возможность хищения, нарушения целостности или уничтожения содержащейся на них информации.

Отчуждаемые съемные носители после окончания работы с ними должны убираться в сейфы или металлические шкафы, запираемые на ключ.

Не допускается оставлять без присмотра на рабочем столе или в СВТ машинные носители, содержащие ПДн.

Персональную ответственность за сохранность полученных машинных носителей и предотвращение несанкционированного доступа к записанным на них ПДн несет работник, за которым закреплен носитель.

6.4. Порядок уничтожения машинных носителей ПДн

Основанием для уничтожения машинных носителей ПДн, является повреждение машинного носителя, исключающее его дальнейшее использование, или потеря практической ценности носителя. Решение об уничтожении машинного носителя принимает должностное лицо ответственное за защиту ПДн.

Списанные машинные носители, подлежащие уничтожению, хранятся в сейфе должностного лица ответственного за защиту ПДн. Уничтожение таких носителей производится раз в год.

Уничтожение носителей производится путем их физического разрушения с предварительным затиранием (форматированием, уничтожением) содержащихся на них ПДн, если это позволяют физические принципы работы носителя.

Уничтожение машинных носителей производится Комиссией в составе не менее 3 человек. В состав Комиссии должно обязательно входить должностное лицо ответственное за защиту ПДн. После уничтожения всех машинных носителей составляется **Акт об уничтожении персональных данных (Приложение Г)**.

При уничтожении, машинные носители снимаются с учета. Отметка об уничтожении носителей проставляется в Журнале.

6.5. Порядок уничтожения (стирания) ПДн с машинного носителя

Основанием для уничтожения (стирания) записей или части записей с электронного носителя являются следующие случаи:

- возврат носителя сотрудником;
- передача носителя в ремонт;
- списание носителя.

Хранящаяся на электронных носителях и потерявшая актуальность информация, содержащая ПДн, своевременно стирается (уничтожается). Работник, совместно с системным администратором Администрации, принимает окончательное решение о необходимости уничтожения (стирания) с него записей.

Работник осуществляет уничтожение информации с носителя самостоятельно, с использованием встроенных средств ОС.

При невозможности самостоятельного уничтожения информации с носителя, работник передает электронный носитель должностному лицу ответственному за защиту ПДн. Совместно с носителем передается служебная записка, в которой указывается причины передачи (возврата) и основание для уничтожения содержащейся на нем информации.

Должностное лицо ответственное за защиту ПДн, ответственное за

уничтожение (стирание) информации с электронных носителей, при получении носителя должно обеспечить уничтожение (стирание) информации с носителя, способом, исключающим ее дальнейшее восстановление и подготовить **Акт об уничтожении персональных данных (Приложение Г)**.

В Акт заносится дата, учетный номер носителя и способ уничтожения (стирания) информации, а также используемые для этого программные средства.

Носители, пригодные к повторной эксплуатации, после уничтожения записанной на них информации могут быть использованы для повторной записи информации.

7. Пересмотр и внесение изменений

Пересмотр положений настоящего документа проводится в следующих случаях:

- при появлении новых требований к обработке и обеспечению безопасности ПДн со стороны законодательства РФ и контролирующих органов исполнительной власти Российской Федерации;
- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;
- не реже одного раза в год.

Ответственным за пересмотр настоящего Порядка и составление рекомендаций по изменению является должностное лицо ответственное за защиту ПДн.

Внесение изменений производится на основании соответствующего распоряжения администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области.

Приложение А

А К Т № _____
о выделении дел и документов, подлежащих уничтожению

от «_____»_____201_ г.

Комиссия в составе:

<Фамилия И.О. – должность;>
<Фамилия И.О. – должность.>
<Фамилия И.О. – должность.>

составила настоящий акт о том, что на основании проведенной экспертизы, отобрала к уничтожению, следующие документы и дела, утратившие практическую ценность:

№ п\п	Заголовок документа\дела	Основание для уничтожения

Члены комиссии:

_____ _____

_____ _____

_____ _____

Приложение Б

А К Т № _____
уничтожения бумажных носителей, содержащих персональные данные

от «_____»_____20__ г.

Комиссия в составе:

<Фамилия И.О. – должность;>
<Фамилия И.О. – должность.>
<Фамилия И.О. – должность.>

составила настоящий акт о том, что произведено плановое уничтожение бумажных носителей, содержащих персональные данные, с истекшим сроком использования и/или утративших практическое значение.

– «тип носителя, учётный номер носителя»
– «тип носителя, учётный номер носителя»
– …

Бумажные носители уничтожены путём сжигания/шредирования/химической обработки и т.п. *(нужное отметить)*.

Члены комиссии

_____ _____

_____ _____

_____ _____

Приложение В

Журнал учета носителей информации, содержащих персональные данные

№ п/п	Учетный № носителя	Дата	Тип носителя	Содержимое носителя	Ф.И.О. отв. лица	Подпись отв. лица	Отметка о возврате (с указанием причины)	Ф.И.О. отв. лица	Подпись отв. лица	Дата уничтожения носителя	Ф.И.О. отв. за уничтожение
1	2	3	4	5	6	7	8	9	10	11	12

Приложение Г

УТВЕРЖДАЮ
_____
Глава муниципального образования
_____
(подпись)
«__» _____ 20__г.

Акт об уничтожении персональных данных

Комиссия в составе:
Председатель – _____
Члены комиссии – _____

провела отбор носителей персональных данных и установила, что в соответствии с требованиями руководящих документов по защите информации _____ информация, записанная на них в процессе эксплуатации, подлежит гарантированному уничтожению:

№ п/п	Дата	Тип носителя	Регистрационный номер носителя ПДн	Примечание

Всего съемных носителей _____
(цифрами и прописью)

На указанных носителях персональные данные уничтожены путем _____.
(стирания на устройстве гарантированного уничтожения информации и т.п.)

Перечисленные носители ПДн уничтожены путем _____.
(разрезания, сжигания, механического уничтожения и т.п.)

Председатель комиссии: _____ /_____/
Члены комиссии: _____ /_____/
_____ /_____/

Приложение № 14

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПОРЯДОК

реагирования на инциденты информационной безопасности в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

1. Термины и определения

В настоящем Порядке использованы следующие термины и определения:

Безопасность персональных данных: Состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Блокирование персональных данных: Временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Вредоносное программное обеспечение: Программное обеспечение, предназначенное для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ к информации: Возможность получения информации и ее использования.

Защита информации: Деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Идентификация: Присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных: Информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таковых средств**.**

Информация: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления**.**

Использование персональных данных: Действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом, затрагивающих права и свободы субъекта ПДн или других лиц**.**

Конфиденциальность персональных данных: Обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта ПДн или наличия иного законного основания.

Несанкционированный доступ (несанкционированные действия): Доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами ПДн.

Обработка персональных данных: Действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение ПДн.

Персональные данные: Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПДн) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь персональных данных: Лицо, участвующее в процессах(е) обработки ПДн или использующее результаты их функционирования.

Процесс обработки персональных данных: Процесс, в котором присутствует обработка персональных данных.

Средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Уничтожение персональных данных: Действия, в результате которых невозможно восстановить содержание ПДн в информационной системе ПДн или в результате которых уничтожаются материальные носители ПДн.

Целостность информации: Способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Доступность информации - Свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.

2. Используемые сокращения

В настоящем Порядке использованы следующие сокращения, приведенные в Таблице 1:

Таблица 1. Сокращения

№ п/п	Сокращение	Описание
1.	**ИБ**	Информационная безопасность
2.	**ИСПДн**	Информационная система ПДн
3.	**НСД**	Несанкционированный доступ
4.	**ПДн**	Персональные данные

3. Область применения

Настоящий Порядок реагирования на инциденты информационной безопасности (далее - Порядок) предназначен для определения единого порядка реагирования на возникшие инциденты информационной безопасности, проведения служебных расследований, а также проведения мероприятий, нацеленных на предотвращение наступления повторных инцидентов в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области (далее по тексту - администрация).

Требования настоящего Порядка распространяются на должностных лиц администрации, отвечающие за обеспечение безопасности ПДн.

4. Общие положения

Настоящий Порядок разработан в соответствии с Политикой администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-фз «О персональных данных».

В соответствии с настоящим Порядком к инцидентам ИБ в администрации относятся:

- нарушение конфиденциальности, целостности или доступности ПДн;

- отказ оборудования, сервисов, средств обработки и (или), входящих в состав ИСПДн;
- несоблюдение требований внутренних организационно-распорядительных документов и действующих нормативных документов РФ в области обработки и защиты ПДн (нарушение правил обработки ПДн);
- заражение программных компонентов ИСПДн вредоносным программным обеспечением.

К инцидентам ИБ в ИСПДн также относятся попытки и факты получения НСД к ИСПДн:
- сеансы работы в ИСПДн незарегистрированных пользователей;
- сеансы работы Пользователей ИСПДн, срок действия полномочий, которых истек, либо в состав полномочий, которых не входят выявленные действия с ПДн;
- действия третьего лица, пытающегося получить доступ (или получившего доступ) с использованием учетной записи другого пользователя в целях получения коммерческой или другой выгоды, методом подбора пароля или иными методами (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.
- совершение попыток несанкционированного доступа к рабочей станции, сейфу, шкафу и др. (нарушение целостности пломб, наклеек с защитной и идентификационной информацией, нарушение или несоответствие номеров печатей и др.);
- несанкционированное внесение изменений в параметры конфигурации программных или аппаратных средств обработки, или защиты, входящих в состав ИСПДн.

Кроме того, к инцидентам ИБ относятся случаи создания предпосылок для возникновения описанных выше инцидентов.

5. Оповещение об инциденте информационной безопасности

В случае выявления инцидента ИБ устанавливается следующая последовательность действий сотрудников администрации:
1) прекратить работу с ресурсом, в котором выявлен инцидент ИБ;
2) оповестить своего непосредственного руководителя о факте выявления инцидента ИБ;
3) руководитель должен оповестить должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн;
4) после извещения указанных должностных лиц по их требованию предоставить всю необходимую информацию.

Должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн проводит краткий анализ произошедшего инцидента ИБ и причин, способствующих его возникновению, и составляет краткую справку, в которой описывается произошедший инцидент ИБ, его последствия и оценка необходимости проведения расследования инцидента ИБ. Справка направляется главе администрации для принятия решения о проведении расследования инцидента ИБ.

Порядок проведения расследования инцидента ИБ описан в разделе 7 настоящего документа.

Мероприятия по устранению причин и недопущению повторного возникновения инцидента ИБ описаны в разделе 8 настоящего документа.

6. Мероприятия при возникновении инцидента информационной безопасности, ставшего причиной возникновения негативных последствий для субъекта ПДн

В случае если инцидент ИБ может стать (или уже стал) причиной возникновения негативных последствий для субъектов ПДн, необходимо немедленно блокировать ПДн этих субъектов до устранения причин, повлекших за собой возникновение инцидента ИБ. Решение о блокировании

ПДн принимает должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн.

ПДн остаются заблокированными до устранения причин, повлекших за собой возникновение инцидента ИБ.

7. Проведение расследования инцидента информационной безопасности

Внутреннее расследование и составление заключений должно в обязательном порядке проводиться в случае выявления:

- нарушения конфиденциальности, целостности или доступности ПДн;
- халатности и несоблюдения требований по обеспечению безопасности ПДн;
- несоблюдения условий хранения носителей ПДн;
- использования СЗИ, которые могут привести к нарушению заданных характеристик безопасности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн.

Задачами внутреннего расследования являются:

- установление обстоятельств нарушения, в том числе времени, места и способа его совершения;
- установление лиц, непосредственно виновных в данном нарушении;
- выявление причин и условий, способствовавших нарушению.

Проведение внутреннего расследования проводится по решению главы муниципального образования. С целью проведения расследования в обязательном порядке формируется Комиссия, в состав которой входят должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн, юрист и иные должностные лица администрации, участие которых может потребоваться.

Комиссия должна приступить к работе по расследованию не позднее следующего рабочего дня после даты выявления инцидента ИБ.

Общая продолжительность внутреннего расследования не должна превышать одного месяца.

В рамках проведения расследования инцидента ИБ Комиссия уполномочена:

- проводить опрос сотрудников администрации, по вине которых предположительно произошел инцидент ИБ, а также должностных лиц, которые могут оказать содействие в установлении обстоятельств возникновения инцидента ИБ;
- проводить осмотр объектов и предметов, которые могут иметь отношение к инциденту ИБ;

По решению главы администрации на Комиссию могут быть возложены дополнительные обязанности и права.

Работник, в отношении которого проводится расследование, должен быть ознакомлен с распоряжением о проведении расследования.

Все действия членов Комиссии и полученные в ходе расследования материалы подлежат письменному оформлению (акты, протоколы, справки и т.п.).

Требование от работника объяснения в письменной форме для установления причины нарушения является обязательным. В случае, когда работник отказывается дать письменные объяснения, его устные показания или отказ от них письменно фиксируются членами Комиссии в виде протокола.

В целях исключения возможности какого-либо воздействия на процесс расследования члены Комиссии обязаны соблюдать конфиденциальность расследования до принятия по нему решения главой администрации.

Для оперативного проведения внутреннего расследования должностное лицо ответственного за защиту ПДн составляет План проведения расследования.

Одновременно с проведением внутреннего расследования, глава администрации может поручить Комиссии определить ущерб для администрации и (или) для субъекта ПДн от произошедшего инцидента ИБ. В

отдельных случаях такая оценка может быть осуществлена с привлечением специализированной организации.

По окончании внутреннего расследования Комиссия представляет главе администрации отчет по результатам расследования, в котором излагаются:

- основания и время проведения расследования;
- проделанная работа (кратко);
- время, место и обстоятельства факта нарушения;
- причины и условия совершения нарушения;
- виновные лица и степень их вины;
- наличие умысла в действиях виновных лиц;
- предложения по возмещению ущерба;
- предлагаемые меры наказания (учитывая личные и деловые качества виновных лиц) или дальнейшие действия;
- рекомендации по исключению подобных нарушений;
- другие вопросы, поставленные перед комиссией (об актуальности конфиденциальной информации, о размерах ущерба и т. д.).

К отчету прилагаются:

- письменные объяснения лиц, которых опрашивали члены Комиссии;
- акты (справки) проверок носителей конфиденциальной информации, осмотров помещений и т. д.;
- другие документы (копии документов), относящиеся к расследованию, в том числе заключения по определению размеров ущерба.

Отчет должен быть подписан всеми членами Комиссии. При несогласии с выводами или содержанием отдельных положений член Комиссии, подписывая заключение, приобщает к нему свое особое мнение (в письменном виде).

Отчет подлежит утверждению главой администрации.

Работник, в отношении которого проводится расследование, или его уполномоченный представитель имеют право ознакомления с материалами расследования и требовать приобщения к материалам расследования представляемых ими документов и материалов.

Работник, в отношении которого проведено расследование, должен быть ознакомлен под роспись с отчетом по результатам расследования.

Решение о привлечении к ответственности работника принимается только после завершения расследования и оформляется приказом.

При наличии в действиях работника признаков административного правонарушения или уголовного преступления глава администрации обязан обратиться в правоохранительные органы для привлечения виновного к ответственности, в соответствии с положениями нормативных документов РФ.

В соответствии с Трудовым кодексом РФ, возмещение ущерба производится независимо от привлечения работника к дисциплинарной, административной или уголовной ответственности за действия или бездействие, которыми причинен ущерб работодателю.

При несогласии работника с результатами подсчета ущерба взыскание должно производиться по решению суда. В этом случае заключение по результатам внутреннего расследования становится письменным обоснованием причастности работника к действиям, повлекшим нанесение ущерба.

Первый экземпляр отчета с резолюцией главы администрации, копия приказа (выписка) по результатам расследования, все материалы внутреннего расследования, включая документ (копию), послуживший поводом для назначения расследования, подлежат хранению в отдельном деле. Дела о внутренних расследованиях хранятся у главы администрации.

8. Превентивные меры по недопущению повторного возникновения инцидентов информационной безопасности

Мероприятия по устранению инцидента ИБ и предупреждающие его повторное возникновение, в зависимости от произошедшего инцидента ИБ, включают в себя:

- мониторинг событий в информационной системе ПДн;

- своевременное удаление неиспользуемых учетных записей;
- контроль и мониторинг действий пользователей в информационной системе ПДн;
- проведение обучения (повторного обучения) пользователей правилам обработки и обеспечения безопасности ПДн;
- ознакомление пользователей с мерами ответственности, установленными нормативными документами РФ, за нарушение норм и правил обработки ПДн, а также за разглашение полученных данных.

9. Пересмотр и внесение изменений

Настоящий Порядок должен пересматриваться в случаях:
- изменения требований законодательства РФ, в области обработки и обеспечения информационной безопасности ПДн;
- по результатам внутреннего контроля (аудита) системы защиты ПДн, в случае выявления существенных нарушений;
- по результатам расследования инцидентов информационной безопасности, связанных с обработкой и обеспечением безопасности ПДн;

Ответственным за пересмотр настоящего Положения и составление рекомендаций по изменению является должностное лицо ответственное за защиту информации и обеспечение безопасности ПДн в администрации.

Внесение изменений производится на основании соответствующего распоряжения администрации.

Приложение № 15

УТВЕРЖДЕНА
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

Инструкция должностного лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в информационных системах персональных данных администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области (далее - ИСПДн).

1.2. Ответственный за организацию обработки персональных данных назначается из числа штатных пользователей ИСПДн, на основании распоряжения администрации «О назначении ответственного за организацию обработки персональных данных в ИСПДн».

1.3. Ответственный за организацию обработки персональных данных в своей работе руководствуется настоящей инструкцией, руководящими и нормативными документами ФСТЭК России и регламентирующими документами ИСПДн.

1.4. Ответственный за организацию обработки персональных данных является должностным лицом, уполномоченным на проведение работ по организации обработки персональных данных в ИСПДн.

2. Обязанности должностного лица, ответственного за организацию обработки персональных данных в ИСПДн

Должностное лицо ответственное за организацию работ по обработке персональных данных обязано:

- взаимодействовать с регулирующими органами по вопросам обработки и обеспечения безопасности персональных данных;
- передавать ответственному за защиту информации ИСПДн информацию по взаимодействию с регулирующими органами в рамках его компетенции;
- контролировать договоры с третьими лицами на предмет их соответствия требованиям организационно-распорядительных документов по обработке и обеспечению безопасности персональных данных;
- предоставлять необходимую информацию при проведении проверок регулирующими органами и при проведении контрольных мероприятий по обеспечению безопасности персональных данных;
- обеспечивать выполнение требований по обработке и обеспечению безопасности персональных данных в соответствии с «Положением о порядке обработки персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области и иными нормативными документами в области обработки и защиты персональных данных;
- осуществлять непрерывный контроль действий, пользователей при обработке персональных данных, разъяснять и требовать от пользователей выполнения требований нормативных документов в области обработки и защиты персональных данных;
- участвовать в процессе разработки организационно-распорядительных документов, регламентирующих требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;
- определять необходимость и направлять на обучение пользователей ИСПДн;

- предоставлять консультации пользователей ИСПДн по вопросам автоматизированной и неавтоматизированной обработки персональных данных в рамках своих компетенций;
- организовывать и контролировать своевременное предоставление пользователями ИСПДн доступа к персональным данным и средствам их обработки в объеме, необходимом для выполнения ими своих трудовых обязанностей;
- определять права доступа к персональным данным и автоматизированным средствам обработки персональных данных в рамках своих компетенций;
- сообщать о выявленных нарушениях требований по обработке персональных данных должностному лицу, ответственному за защиту информации;
- обеспечивать выполнение плана периодических проверок условий обработки персональных данных в пределах своих функциональных обязанностей;
- участвовать в разработке плана периодических проверок условий обработки персональных данных.

3. Права должностного лица, ответственного за организацию обработки персональных данных в ИСПДн

Должностное лицо, ответственное за организацию работ по обработке персональных данных, имеет право:
- формировать предложения по совершенствованию системы защиты информации для должностного лица, ответственного за защиту информации, обрабатываемой в ИСПДн;
- формировать предложения о необходимости проведения контрольных мероприятий по обеспечению безопасности персональных данных для должностного лица, ответственного за защиту информации;
- формировать предложения по внесению изменений в организационно-распорядительные документы, регламентирующие требования по обеспечению информационной безопасности персональных данных, обрабатываемых в ИСПДн;
- организовывать проведение периодических проверок условий обработки персональных данных;
- осуществлять ознакомление служащих, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных;
- в случаях, установленных нормативными правовыми актами Российской Федерации, в соответствии с требованиями и методами, установленными уполномоченным органом по защите прав субъектов персональных данных, осуществлять обезличивание персональных данных, обрабатываемых в ИСПДн.

4. Нештатные ситуации

В случае возникновения нештатных ситуаций ответственный за организацию обработки персональных данных обязан незамедлительно принять все необходимые меры по устранению причины возникновения нештатной ситуации для минимизации ее последствий.

В случае возникновения нештатных ситуаций ответственный за организацию обработки персональных данных обязан немедленно оповестить руководство о нештатной ситуации.

В случае возникновения нештатных ситуаций ответственный руководствуется Инструкцией по порядку резервирования и восстановления работоспособности технических (аппаратных) средств, программного обеспечения, баз данных и средств защиты информации в ИСПДн.

5. Ответственность

На лицо, ответственное за организацию обработки персональных данных, возлагается персональная ответственность за организацию обработки

персональных данных в ИСПДн в соответствии с функциональными обязанностями.

Лицо, ответственное за организацию обработки персональных данных, несет ответственность по действующему законодательству за разглашение информации ограниченного доступа, ставшей известной ему по роду работы.

Приложение № 16

УТВЕРЖДЕНА
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

Инструкция
пользователя информационной системы персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

Сокращения

Сокращение	Расшифровка
АРМ	автоматизированное рабочее место
ИСПДн	информационная система персональных данных
ПДн	персональные данные

1. Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку ПДн в ИСПДн, используемых в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области (далее - администрация).

1.2. Пользователем является каждый сотрудник администрации, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность согласно действующему законодательству Российской Федерации за свои действия и за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, Положением об обработке и защите ПДн, руководящими и нормативными документами ФСТЭК России и ФСБ России и регламентирующими документами администрации.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение безопасности ПДн.

2. Должностные обязанности

Пользователь **обязан**:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на АРМ только те процедуры, которые определены для него Положением о разрешительной системе допуска пользователей и обслуживающего персонала к информационным ресурсам и системе защиты персональных данных.

2.3. Знать и соблюдать установленные требования по режиму обработки ПДн, учету, хранению и пересылке носителей информации, защите ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключить возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью администрации, а так же для получений консультаций по вопросам информационной безопасности, необходимо обращаться к системному администратору Администрации.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к системному администратору Администрации.

2.9. Пользователям **запрещается**:

- - разглашать защищаемую информацию третьим лицам;
- - копировать защищаемую информацию на внешние носители без разрешения Ответственного за организацию обработки ПДн;
- - самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- - несанкционированно открывать общий доступ к папкам на своем АРМ;
- - запрещено подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства;
- - отключать (блокировать) средства защиты информации;
- - обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- - сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки АРМ.

2.10. При отсутствии визуального контроля за АРМ доступ к нему должен быть немедленно заблокирован.

2.11. Принимать меры по реагированию, в случае возникновения внештатных или аварийных ситуаций, с целью ликвидации их последствий, в рамках и пределах возложенных на него функций.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются Пользователям системным администратором Администрации (Администратором ИСПДн).

3.2. Полная плановая смена паролей в ИСПДн проводится системным администратором Администрации (администраторами ИСПДн).

3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.4. Правила хранение пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим Пользователям личный пароль и регистрировать их в системе под своим паролем.

3.5. Лица, использующие паролирование, **обязаны**:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети **запрещается**:

- осуществлять работу при отключенных средствах защиты (антивирус и др.);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- посещать Интернет-ресурсы, содержащие информацию экстремистского, расистского, порнографического и криминального характера, а также загружать данные, содержащие подобную информацию;
- использовать адрес корпоративной почты при регистрации на Интернет-ресурсах, в ходе деятельности, не связанной с выполнением должностных обязанностей;
- скачивать из Сети медиа-файлы развлекательного характера, программное обеспечение и другие файлы;
- размещать в сети Интернет информацию, классифицированную как «для служебного пользования», «персональные данные», «коммерческая тайна»;

4.3. Ответственный за организацию обработки ПДн оставляет **за собой право**:

- осуществлять мониторинг использования сотрудниками администрации сети Интернет;
- определять перечень запрещенных Интернет-ресурсов и осуществлять блокировку доступа к ним;
- осуществлять мониторинг появления адресов корпоративной почты на страницах Интернет-ресурсов;
- осуществлять мониторинг появления информации конфиденциального характера о деятельности администрации в сети Интернет, в том числе и на страницах социальных сетей, таких как www.vk.com, www.odnoklassniki.ru и др.;
- предоставлять информацию об использовании Интернет-ресурсов сотрудниками администрации правоохранительным органам в случаях, предусмотренных законодательством Российской Федерации;
- принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей инструкции.

5. Правила работы с корпоративной электронной почтой

5.1 Электронная почта является собственностью администрации и может быть использована **ТОЛЬКО** в служебных целях. Использование электронной почты в других целях категорически **ЗАПРЕЩЕНО**.

5.2 Содержимое электронного почтового ящика сотрудника может быть проверено без предварительного уведомления по требованию главы администрации.

5.3 При работе с корпоративной системой электронной почты сотрудникам компании **запрещается**:

- - использовать адрес корпоративной почты для оформления подписок, без предварительного согласования с главой администрации;
- - публиковать свой адрес, либо адреса других сотрудников компании на общедоступных Интернет ресурсах (форумы, конференции и т.п.);
- - отправлять сообщения с вложенными файлами общий объем которых превышает 5 Мегабайт.
- - открывать вложенные файлы во входящих сообщениях без предварительной проверки антивирусными средствами, даже если отправитель письма хорошо известен;
- - осуществлять массовую рассылку почтовых сообщений внешним адресатам без их на то согласия. Данные действия квалифицируются как СПАМ и являются незаконными;
- - осуществлять массовую рассылку почтовых сообщений рекламного характера;

- рассылка через электронную почту материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также ссылки на вышеуказанную информацию;
- - распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны.
- - распространять информацию содержание и направленность которой запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и т.д.
- - распространять информацию ограниченного доступа, представляющую коммерческую тайну;
- - предоставлять, кому быто ни было пароль доступа к своему почтовому ящику.

6. Порядок действия пользователя при возникновении инцидента информационной безопасности

- При выходе из строя СЗИ необходимо:
- - немедленно прекратить обработку информации на объекте;
- - обратиться к администратору информационной безопасности.
- При выходе из строя составных частей ИСПДн:
- - немедленно прекратить обработку информации на объекте;
- - обратиться к администратору информационной безопасности.

7. Ответственность пользователя

На пользователя возлагается персональная ответственность за соблюдение установленного режима защиты информации ограниченного распространения в соответствии с его функциональными обязанностями, определенными настоящей Инструкцией.

Пользователь несет ответственность в соответствии с действующим законодательством РФ за нарушение требований настоящей Инструкции.

Приложение № 17

УТВЕРЖДЕНЫ
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

Границы контролируемой зоны

информационных систем персональных данных в администрации муниципального образования «Агалатовское сельское поселение» Всеволожского муниципального района Ленинградской области

Границы контролируемой зоны по адресу:

Ленинградская область, Всеволожский район, д. Агалатово, в/г дом 158, 2 этаж

Границы контролируемой зоны проходят по периметру 2 этажа, в пределах которого исключено присутствие посторонних лиц без допуска.

Ленинградская область, Всеволожский район, д. Агалатово, в/г дом 160, 3 этаж, кабинет паспортного стола

Контролируемая зона включает пространство здания или *этажа*, *кабинета* в котором исключено неконтролируемое пребывание работников (сотрудников) оператора и лиц, не имеющих постоянного допуска к объектам информационной системы персональных данных, а также транспортных, технических и иных материальных средств.

Приложение № 18

УТВЕРЖДЕН
распоряжением администрации МО
«Агалатовское сельское поселение»

от 31 августа 2021 № 81

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Понятие информационной системы персональных данных.

Информационная система персональных данных — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2. Информационные системы персональных данных:

— «Кодекс: Документооборот» (СЭД «Единая система электронного делопроизводства и документооборота»;

— Автоматизированная информационная система «Межвед ЛО» портал СМЭВ Ленинградской области;

— «Контур–Экстерн»;

— «1С: Предприятие 8.2. Зарплата и кадры бюджетного учреждения»;

— «АЦК-Планирование»;

— АС «Сбербанк Бизнес Онлайн» (СББОЛ);

— «АЦК-Финансы»;

— «АЦК-Закупки»;

— «СУФД»;

— ИАС «Поселение»